LOWER BOUNDS FOR THE CIRCUIT SIZE OF PARTIALLY HOMOGENEOUS POLYNOMIALS

HÔNG VÂN LÊ

Abstract. In this note we introduce a class of weakly elusive functions, which is slightly larger than the class of elusive functions introduced by Raz. We introduce the notion of partially homogeneous polynomials, which encompasses all homogeneous multilinear polynomials, e.g. the permanent and the determinant. We obtain lower bounds for the circuit size of a partially homogeneous polynomial in terms of the weak elusiveness of a family of polynomial mappings associated with the polynomial in consideration. We discuss several algebraic methods for proving that a polynomial mapping is weakly elusive.

AMSC: 03D15, 68Q17, 13P25

Contents

1. Introduction 2
2. (s, r)-weakly elusive functions 3
3. Estimating the circuit size of the permanent (or a partially homogeneous polynomial) from below 5
3.1. Lower bounds for the circuit size of the permanent 5
3.2. Lower bounds for the circuit size of a partially homogeneous polynomial 6
4. Algebraic methods for proving that a polynomial mapping is weakly elusive 8
4.1. Counting the dimension of the space of regular functions 8
4.2. Reduction 10
4.3. Geometry of the mapping $\tilde{g}^{n,t}$ associated to the permanent 12
5. Appendix: Normal form of arithmetic circuits and universal circuit-graph 13
Acknowledgements 17
References 17

H.V.L. is supported by RVO: 67985840.

1. Introduction

Let $\mathbb{F}$ be a field. Recall that the permanent $P_n(\mathbb{F}) \in \mathbb{F}[x_{ij}|\, 1 \leq i,j \leq n]$ is defined by

$$P_n([x_{ij}]) := \sum_{\sigma \in \Sigma_n} \Pi_{i=1}^n x_{i\sigma(i)}.$$

Finding non-trivial lower bounds for the circuit size or formula size of the permanent P_n is a challenging problem in algebraic computational complexity theory, especially in understanding the VP versus VNP problem [2], [3], [10], [8]. It has been pointed out by Mulmuley-Sohoni [6] that a proof of $VP \neq VNP$ which is based on a generic property of $poly(n)$-definable polynomials will likely fall in the trap of the "natural proof". On the other hand, proving that a sequence of polynomials of large circuit size (resp. formula size) is $poly(n)$-definable seems to be equally hard as proving a non-trivial lower bound for the circuit size (resp. the formula size) of the permanent, since the permanent is VNP-complete. Up to now, there is no known tool for obtaining a non-trivial lower bound for the circuit size of the permanent. The only known tool for obtaining a non-trivial lower bound for the formula size of the permanent exploits the Valiant theorem on the relation between the formula size and the determinantal complexity of the permanent [9], [5], [6]. The determinantal complexity c_{det}, though better understood than the formula size, is still very complicated. The best lower bound $c_{det}(P_n) \geq (n^2/2)$ has been obtained by Mignon and Ressayer [5]. To get the quadratic estimate, Mignon and Ressayer compared the curvature of the hypersurfaces $\{\det_m(x) = 0\}$ and $\{Per_n(x) = 0\}$. Mulmuley and Sohoni suggested to use representation theory to obtain lower bounds for $c_{det}(P_n)$ [6].

In [7] Raz proposed a method of elusive functions to construct polynomials of large circuit size. He emphasized that the hard problem is to construct polynomials of large circuit size which are also $poly(n)$-definable.

In this note, exploiting Raz's idea, we associate the permanent P_n with a family of homogeneous polynomial mappings $g^{n,t} : \mathbb{F}^{(t-1)n} \to \mathbb{F}^{n\binom{(n+1)(n-t)-1}{n-t}}$ of degree $t-1$ and with a family of homogeneous polynomial mappings $\tilde{g}^{n,t} : \mathbb{F}^{tn} \to \mathbb{F}^{\binom{n}{n-t}}$ of degree t. Here $t \in [2, n-2]$ is a parameter. We obtain a lower bound for the circuit size of the permanent P_n in terms of either the weak elusiveness of $g^{n,t}$ (Theorem 3.1) as of the weak elusiveness of $\tilde{g}^{n,t}$ (Theorem 3.3, Example 3.6). We also extend the above method to obtain lower bounds for the circuit size of a partially homogeneous multivariate polynomial.

The plan of our note is as follows. In section 2 we introduce the notion of weakly elusive functions. In section 3 we prove our main result relating the circuit size of the permanent (or any partially homogeneous polynomial) with the weak elusiveness of associated polynomial mappings. In section 4 we discuss several methods for proving the weak elusiveness of a polynomial mapping, and using them to construct new examples of weakly elusive functions. In the appendix we reformulate a normal form theorem and the existence of a universal circuit-graph, which are originally due to Raz, in the form that is needed for our note.

For the sake of simplicity of the exposition, we assume in this note that $\mathbb{F}$ is a field of characteristic 0. Then any polynomial $f \in \mathbb{F}[x_1, \cdots, x_n]$ can be identified with the associated polynomial function $f : \mathbb{F}^n \to \mathbb{F}$. In the same way, we identify an ordered m-tuple of polynomials $g_1, \cdots, g_m \in \mathbb{F}[x_1, \cdots, x_n]$ with the associated polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$. The space of all polynomials of degree at most r on $\mathbb{F}^n$ will be denoted by $Pol^r(\mathbb{F}^n)$, and the space of all polynomial mappings from $\mathbb{F}^n$ to $\mathbb{F}^m$ of degree at most r will be denoted by $Pol^r(\mathbb{F}^n, \mathbb{F}^m)$.

2. (s, r)-weakly elusive functions

In this section we introduce the notion of an (s, r)-weakly elusive function (Definition 2.1), which is slightly weaker than the notion of an (s, r)-elusive function introduced by Raz (Example 2.2). Then we show how this notion measures the circuit size of a polynomial family of m-tuples of homogeneous polynomials (Proposition 2.4). The key notion is a polynomial family of homogeneous polynomial mappings (Definition 2.3).

Definition 2.1. (cf. [7, Definition 1.1]) A polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ is called (s, r)-*weakly elusive*, if its image does not belong to the image of any homogeneous multilinear polynomial mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r.

Example 2.2.
(1) Any (s, r)-elusive polynomial mapping is (s, r)-weakly elusive.
(2) The curve $(1, x, \cdots, x^m) \in \mathbb{R}^{m+1}$ is $(m, 1)$-weakly elusive, since its image does not belong to any hyper-surface through the origin of $\mathbb{R}^{m+1}$. On the other hand, this curve is not $(m, 1)$-elusive, since it lies on the affine hyper-surface $x_1 = 1$ in $\mathbb{R}^{m+1}$.

The notion of (s, r)-weakly elusive functions is useful, when we want to verify, whether a polynomial family of homogeneous polynomial mappings has uniformly bounded circuit size.

Let us fix some notations.

- For any $p, n, m \in \mathbb{N}$ let $Pol^p_{hom}(\mathbb{F}^n)$ denote the space of homogeneous polynomials of degree p on $\mathbb{F}^n$ and $Pol^p_{hom}(\mathbb{F}^n, \mathbb{F}^m)$ the space of homogeneous polynomial mappings of degree p from $\mathbb{F}^n$ to $\mathbb{F}^m$.
- Given a set S of variables $x_1, \cdots, x_l$ we denote by $\mathbb{F}\langle S\rangle$ the vector space $\mathbb{F}^l$ with coordinates $x_1, \cdots, x_l$.

Definition 2.3. A family $F_\lambda \in Pol^r_{hom}(\mathbb{F}^n, \mathbb{F}^m)$, $\lambda \in \mathbb{F}^k$, is called *a polynomial family of homogeneous polynomial mappings*, if there exists a polynomial mapping $f : \mathbb{F}^k \to \mathbb{F}^N$, $N = \dim Pol^r_{hom}(\mathbb{F}^n, \mathbb{F}^m)$, such that $F_\lambda = f(\lambda)$ for all $\lambda \in \mathbb{F}^k$. The polynomial mapping f is called *associated with the family* F_λ.

Proposition 2.4. *Let $Z = \{z_1, \cdots, z_n\}$ be a set of variables, $n \leq s$ and $m \leq 32s(r+1)^2$. Assume that $F_\lambda \in Pol^r_{hom}(\mathbb{F}\langle Z\rangle, \mathbb{F}^m) = (Pol^r_{hom}\langle Z\rangle)^m$, $\lambda \in \mathbb{F}^k$, is a polynomial family of homogeneous polynomial mappings such that for each $\lambda \in \mathbb{F}^k$ the circuit size of F_λ is at most s. Then the associated polynomial mapping f is not $(l, 2r-1)$-weakly elusive for any $l \geq l_0 := s^2 \cdot 2^8 r^2 (r+1)^4$.*

Proof. To prove Proposition 2.4 it suffices to show the existence of a homogeneous multilinear polynomial mapping

$$\Gamma_G : \mathbb{F}^l \to (Pol^r_{hom}(\mathbb{F}\langle Z\rangle))^m$$

such that

$$f(\mathbb{F}^k) \subset \Gamma_G(\mathbb{F}^l). \tag{2.1}$$

The polynomial Γ_G is constructed using Proposition 5.5 which asserts the existence of a universal circuit-graph $G_{s,r,n,m}$ for homogeneous polynomial mappings $P \in Pol^r_{hom}(\mathbb{F}^n, \mathbb{F}^m) = (Pol^r_{hom}(\mathbb{F}\langle Z\rangle))^m$ such that P is of circuit size at most s. By Proposition 5.5 $G_{s,r,n,m}$ has at most l_0 edges leading to the sum-gates. We label these edges with $y_1, \cdots, y_{\bar{l}}$, where $\bar{l} \leq l_0$. We label the other edges of $G_{s,r,n,m}$ with the field element 1. Now we define Γ_G to be the polynomial mapping in the variables $y_1, \cdots, y_l$ such that

$$\Gamma_G(\alpha_1, \cdots, \alpha_l) = (g_1, \cdots, g_m)$$

where $(g_1, \cdots, g_m)$ are the m output-gates of the circuit $\Phi_{G_{s,r,n,m}}$ obtained from $G_{s,r,n,m}$ by replacing the label y_i with the field element $\alpha_i \in \mathbb{F}$ for all $i \in [1, \bar{l}]$. (Thus Γ_G depends only in $\bar{l}$ variables.) Clearly the polynomial mapping Γ_G is multilinear and homogeneous of degree $2r-1$ (cf. [7, Proposition 3.2]). By the assumption of Proposition 2.4 for any $\lambda \in \mathbb{F}^n$ the circuit size of $f(\lambda)$ is at most s. Taking into

account Proposition 5.5, there exists $\alpha \in \mathbb{F}^l$ such that $f(\lambda) = \Gamma_G(\alpha)$. This proves (2.1) and completes the proof of Proposition 2.4. □

Remark 2.5. Proposition 2.4 implies that a polynomial family $F_\lambda \in Pol^r_{hom}(\mathbb{F}^n, \mathbb{F}^m)$, $\lambda \in \mathbb{F}^k$, has a member with circuit size greater than or equal $s+1$ if the associate polynomial mapping $f : \mathbb{F}^k \to Pol^r_{hom}(\mathbb{F}^n, \mathbb{F}^m)$ is $(l, 2r-1)$-weakly elusive, where $l \geq s^2 \cdot 2^8 r^2 (r+1)^4$. In the section 4 we will discuss several methods to prove that a polynomial mapping is weakly elusive.

3. Estimating the circuit size of the permanent (or a partially homogeneous polynomial) from below

In this section we introduce the notion of a partially homogeneous multivariate polynomial (Definition 3.2), whose example is the permanent. We attach to the permanent (resp. a partially homogeneous polynomial) a polynomial family of homogeneous polynomial mappings. We estimate from below the circuit size of the permanent (resp. a partially homogeneous polynomial) in terms of the weak elusiveness of the associated polynomial mapping (Theorem 3.1, Theorem 3.4).

3.1. Lower bounds for the circuit size of the permanent.

Throughout this subsection n is a basic parameter.

We fix an additional parameter $2 \leq t \leq n-2$. Then we partition the set of variables $\{x_{ij}, 1 \leq i, j \leq n\}$ into three subsets X, Y, Z as follows

$$X = \{x_{1i},\, i \in [1,n]\},$$

$$Y = \{x_{ki},\, 2 \leq k \leq t,\, i \in [1,n]\},$$

$$Z = \{x_{ki},\, t+1 \leq i \leq n,\, i \in [1,n]\}.$$

We represent the permanent as follows

$$P_n([x_{ij}]) = \sum_{i=1}^{n} x_{1i} P_{n-1,i}(Y,Z), \tag{3.1}$$

where $P_{n-1,i}(Y,Z)$ is the homogeneous polynomial of degree $n-1$ that is defined uniquely by (3.1). Now we introduce some notations used in this subsection.

(1) Set $m' := \dim Pol^{n-t}_{hom}(\mathbb{F}\langle Z\rangle) = \binom{(n-t)(n+1)-1}{n-t}$.
(2) Set $m := n \cdot m'$.
(3) Let $h : [1, m'] \to Pol^{n-t}_{hom}(\mathbb{F}\langle Z\rangle)$ be an ordering of the monomial basis.

(4) For each $i \in [1, n]$ there is a unique decomposition

$$P_{n-1,i}(Y, Z) = \sum_{j=1}^{m'} f_{j,i}^{n-1}(Y)h(j),$$

where $f_{j,i}^{n-1}(Y)$ is a homogeneous polynomial of degree $t-1$ in Y.

(5) We define a polynomial mapping

$$g^{n,t} : \mathbb{F}\langle Y\rangle \to (Pol_{hom}^{n-t}(\mathbb{F}\langle Z\rangle))^n$$

by determining its (j, i)-coordinate component $g_{j,i}^{n,t}$, for all $i \in [1, n]$ and $j \in [1, m']$, as follows

$$g_{j,i}^{n,t}(x_{21}, \cdots, x_{tn}) := f_{j,i}^{n-1}(x_{21}, \cdots, x_{tn})h^{-1}(j). \tag{3.2}$$

Theorem 3.1. *Assume that the polynomial mapping $g^{n,t}$ defined in (3.2) is $(s, 2(n-t)-1)$-weakly elusive. Then the circuit size $L(P_n)$ of the permanent P_n satisfies*

$$L(P_n) > \frac{\sqrt{s}}{5 \cdot 2^4(n-t)(n-t+1)^2}.$$

Proof. Assume the opposite i.e., $L(P_n) \leq l := \frac{\sqrt{s}}{2^4(n-t)(n-t+1)^2}$. Note that $P_{n-1,i}$ is the partial derivative of P_n in the variable x_{1i}. By the Baur-Strassen result [1], there exists an arithmetic circuit of size less than $5l$ that computes the n-tuple

$$DP_n(Y, Z) := \{P_{n-1,i}(Y, Z) \in Pol^{n-1}(\mathbb{F}^{(n-1)n}) |\, i \in [1, n]\}.$$

Note that for any value $a = (a_{21}, \cdots, a_{tn}) \in \mathbb{F}\langle Y\rangle$ we have

$$g^{n,t}(a) = DP_n(a, Z),$$

which is an n-tuple of polynomials in Z of circuit size less than or equal to $L(DP_n)$. Since $L(DP_n) < 5l$, we obtain

$$L(g^{n,t}(a)) < 5l \text{ for all } a \in \mathbb{F}\langle Y\rangle.$$

Using Proposition 2.4 (or Remark 2.5) we complete the proof of Theorem 3.1. □

3.2. **Lower bounds for the circuit size of a partially homogeneous polynomial.**

Definition 3.2. A multivariate polynomial $P \in \mathbb{F}[x_1, \cdots, x_n]$ is called *partially homogeneous*, if there exists a non-empty set Z of variables $(x_1, \cdots, x_n)$ such that f is homogeneous in Z.

For example, any homogeneous multilinear polynomial is partially homogeneous.

Let $P \in \mathbb{F}[x_1, \cdots, x_n]$ be homogeneous in the subset Z of its variables. Set

$$Z^{\perp} := \{x_1, \cdots, x_n\} \setminus Z.$$

Let X be a subset of $Z^{\perp}$ such that for each $x_i \in X$ the polynomial P has exactly degree 1 in x_i. This set X maybe empty and need not to be the subset of all variables x_j of degree 1 in P.

Let

- $Y := Z^{\perp} \setminus X$;
- $k := \#(Z)$ and $p := \#(X)$;
- r the total degree of P in Z;
- $m' := \dim Pol^r_{hom}(\mathbb{F}\langle Z\rangle) = \binom{k+r-1}{r}$;
- $m := m'$ if X is an empty set. If not, set $m := p \cdot m'$;
- $h : [1, m'] \to Pol^r_{hom}(\mathbb{F}\langle Z\rangle)$ an ordering of the monomial basis.

(1) Assume that X is an empty set. Then P is a polynomial in variables Y, Z. Write

$$P := \sum_{j=1}^{m} P_{j,0}(Y)h(j).$$

We define a polynomial mapping $\tilde{P} : \mathbb{F}\langle Y\rangle \to Pol^r_{hom}(\mathbb{F}\langle Z\rangle)$ as follows

$$\tilde{P}(a) := \sum_{j=1}^{m} P_{j,0}(a)h(j).$$

(2) Assume that $p \geq 1$. Let us enumerate the polynomials in the set $\{\frac{\partial P}{\partial x}, x \in X\}$ by $P_1, \cdots, P_p$. Write

$$P_j(Y, Z) := \sum_{j=1}^{m'} f_{j,i}(Y)h(j).$$

We define a polynomial mapping $\tilde{P} : \mathbb{F}\langle Y\rangle \to (Pol^r_{hom}(\mathbb{F}\langle Z\rangle))^p$ as follows

$$\tilde{P}(a) := \sum_{i=1}^{p} \sum_{j=1}^{m} P_{j,i}(a)h(j).$$

The following Theorem is proved in the same way as Theorem 3.1, so we omit its proof.

Theorem 3.3. *Assume that the polynomial mapping $\tilde{P}$ defined by the recipe above is $(s, 2r-1)$-weakly elusive. Then the circuit size $L(P)$ of*

P satisfies

$$L(P) > \frac{\sqrt{s}}{5 \cdot 2^4 r(r+1)^2},$$

if X is not an empty set

Next, we estimate the circuit size of arithmetic circuits with bounded depth that compute a special partially homogeneous polynomial P.

Theorem 3.4. *Assume that P is linear in each of the variable in Z and $\frac{p \cdot k}{n} > 1$. If the polynomial map $\tilde{P} : \mathbb{F}\langle Y\rangle \to (\mathbb{F}\langle Z\rangle)^p$ is (s,d)-weakly elusive, then the circuit size of any depth-$\lfloor \frac{d}{3} \rfloor$ arithmetic circuit that computes P is at least $s/5$.*

Proof. This Theorem is an analogue of Raz's theorem [7, Proposition 3.11], where Raz assume that $p \cdot k = n^2$. It is based on the following

Lemma 3.5. *(cf.* [7, Proposition 3.4]*) Assume that G is the circuit-graph in a normal-linear-form. Then the associated mapping Γ_G is a polynomial mapping of degree $Depth(G)$.*

This Lemma differs from [7, Proposition 3.4] only in Raz's assumption that $k \cdot p = n^2$, which does not affect his proof, so we omit it. Now we complete the proof of Theorem 3.4 in the same way as the proof of Theorem 3.1. □

Example 3.6. We return to the permanent P_n, keeping the notation in subsection 3.1. The polynomial mapping $g^{n,t}$ constructed in subsection 3.1 is a prototype of the polynomial mapping $\tilde{P}$ constructed in subsection 3.2.(2). Now we attach to the permanent another family of polynomial mappings $\tilde{g}^{n,t} : \mathbb{F}\langle X, Y\rangle \to Pol^{n-t}_{hom}(\mathbb{F}\langle Z\rangle)$, using the recipe in 3.2.(1). We determine the j-th coordinate $\tilde{g}^{n,t}_j$ of $\tilde{g}^{n,t}$ as follows

$$\tilde{g}^{n,t}_j(X,Y) := \tilde{f}^{n-1}_j(X,Y)h(j).$$

Here $\tilde{f}^{n,t}_j(X,Y)$ is defined unique from the equation

$$Per_n(X,Y,Z) = \sum_{j=1}^{m'} \tilde{f}^{n-1}_j(X,Y)h(j).$$

4. Algebraic methods for proving that a polynomial mapping is weakly elusive

4.1. **Counting the dimension of the space of regular functions.** For a given quadruple (s,r,m,d) with $s \leq m-1$ let us denote by

- $L(s,r,m,d)$ the space of all polynomials g on $\mathbb{F}^s$ which can be written as

$$g = \Gamma^*(f) \text{ (i.e., } g(y) = f(\Gamma(y)) \text{ for all } y \in \mathbb{F}^s), \tag{4.1}$$

  where $f \in Pol^d(\mathbb{F}^m)$ and Γ is a multilinear homogeneous polynomial mapping of exactly degree r from $\mathbb{F}^s$ to $\mathbb{F}^m$;
- $L_{hom}(s,r,m,d)$ the subspace in $L(s,r,m,d)$ consisting of those g defined by (4.1) where $f \in Pol^d_{hom}(\mathbb{F}^m)$;
- $Pol^{rd,d}_{(hom)}(\mathbb{F}^s)$ the set of all (homogeneous) of degree rd polynomials g in $(x_1, \cdots, x_s)$ such that the degree of g in each variable s_i does not exceed d.

It is easy to check that

$$\dim L_{hom}(s,r,m,d) \le \dim Pol^{rd,d}_{hom} < \min\{\binom{\binom{s}{r}+d-1}{d}, \binom{s+rd-1}{rd}\}, \tag{4.2}$$

$$\dim L(s,r,m,d) \le \dim Pol^{rd,d}_{hom} < \min\{\binom{\binom{s}{r}+d}{d}, \binom{s+rd}{rd}\}. \tag{4.3}$$

In this subsection we assume that P is a polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^m$, where $m \ge n+1 \ge 3$.

- Denote by $A^d_{hom}(P)$ the quotient space $Pol^d_{hom}(\mathbb{F}^m)/I^p_{hom}(P(\mathbb{F}^n))$, where $I^p_{hom}(P(\mathbb{F}^n))$ consists of all homogeneous polynomials of exactly degree d in the ideal $I(P(\mathbb{F}^n))$;
- Denote by $A^d(P)$ the quotient space $Pol(\mathbb{F}^m)/I^p(P(\mathbb{F}^m))$, where $I^p(P(\mathbb{F}^n))$ is the subset of $I(P(\mathbb{F}^n))$ consisting of polynomials of degree not greater than p.

Proposition 4.1. *Assume that for some $d \ge 1$ one of the following two conditions holds*

(1) $\dim A^d_{hom}(P) > \dim L_{hom}(s,r,m,d)$,
(2) $\dim A^d(P) > \dim L(s,r,m,d)$.

Then P is (s,r)-weakly elusive.

Proof. Assume that P satisfies the condition (1) of Proposition 4.1. We will show that for any homogeneous multilinear mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r the image of P does not lie on the image of Γ. Assume the opposite, i.e. there exists a homogeneous multilinear mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r such that $P(\mathbb{F}^n) \subset \Gamma(\mathbb{F}^s)$. Then

$$I_{hom}(\Gamma(\mathbb{F}^s)) \subset I_{hom}(P(\mathbb{F}^n)). \tag{4.4}$$

Let $I^{\perp,d}_{hom}(P(\mathbb{F}^n))$ be a complement of the subspace $I^d_{hom}(P(\mathbb{F}^n))$ in $Pol^d_{hom}(\mathbb{F}^m)$. Since Γ is multilinear homogeneous of degree r we have

(4.5)
$$\dim \Gamma^*(I^{\perp,d}_{hom}(P(\mathbb{F}^n))) \leq \dim \Gamma^*(Pol^d_{hom}(\mathbb{F}^m)) \leq \dim L_{hom}(s,r,m,d).$$

On the other hand, by (4.4), we have

$$\dim \Gamma^*(I^{\perp,d}_{hom}(P(\mathbb{F}^n))) = \dim A^d_{hom}(P). \tag{4.6}$$

Clearly (4.5) and (4.6) contradict the assumption of our Proposition. This proves that P is (s,r)-weakly elusive.

In the same way we prove that P is (s,r)-weakly elusive, if the condition (2) in Proposition 4.1 holds. This completes the proof of Proposition 4.1. □

Example 4.2. Let us consider the Veronese mapping $\nu_k : \mathbb{C}^n \to \mathbb{C}^{\binom{n+k-1}{k}}$ of degree k. It is known that the ideal of the image of the Veronese mapping is generated by quadratic homogeneous functions on $\mathbb{C}^{\binom{n+k-1}{k}}$. Hence $\dim A^1_{hom}(\nu_k) = \binom{n+k-1}{k}$. By Proposition 4.1, taking into account (4.2), ν_k is (n^α, r)-weakly elusive, if

$$\binom{n+k-1}{k} \geq \binom{n^\alpha}{r} + 1.$$

Remark 4.3. The methods presented in this subsection is an extension/modification of the Raz's method in [7] for his study of elusive functions. Using similar ideas, Raz constructed elusive functions, and consequently, obtained non-trivial lower bounds for the size of arithmetic circuits with constant depth computing certain homogeneous polynomials. A careful analysis shows that the counting dimension method has its limitation in proving lower bounds for the circuit size of polynomials, if one uses only (weakly) elusive functions. For example, it is impossible to prove any non-trivial lower bound for the permanent using (weakly) elusive functions, based on the counting dimension argument.

4.2. **Reduction.** As in [4] we reduce the problem of verifying whether a polynomial mapping $P : \mathbb{F}^n \to \mathbb{F}^m$ is (s,r)-weakly elusive, to verifying whether a subset A in the image of $P(\mathbb{F}^n)$ is (s,r)-weakly elusive.

Definition 4.4. A subset $A \subset \mathbb{F}^m$ is called (s,r)-*weakly elusive*, if A does not lie on any image of a homogeneous multilinear polynomial mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r.

In order to prove that P is (s,r)-weakly homogeneous, it suffices to show the existence of a k-tuple of points in the image of $P(\mathbb{F}^n)$, which

is (s,r)-homogeneously elusive, i.e. it does not lie on the image of any homogeneous polynomial $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r. As in [4] we identify a k-tuple $S_k = (b_1, \cdots, b_k)$, $b_i \in \mathbb{F}^m$, with the point $\bar{S}_k \in (\mathbb{F}^m)^k$.

Denote by $(\Lambda^r(\mathbb{F}^s)^*)^m$ the space of multilinear homogeneous polynomial mappings of exactly degree r from $\mathbb{F}^s$ to $\mathbb{F}^m$.

Proposition 4.5. *(cf.* [4, Lemma 2.4]*) A tuple S_k of k points in $\mathbb{F}^m$ is (s,r)-weakly elusive, if and only if $\bar{S}_k$ does not belong to the image of the evaluation map*

$$\bar{E}v^k_{s,r,m} : (\Lambda^r(\mathbb{F}^s)^*)^m \times (\mathbb{F}^s)^k \to (\mathbb{F}^m)^k,$$

$$((f_1, \cdots, f_m), (a_1, \cdots, a_k)) \mapsto (f_1(a_1), \cdots, f_m(a_k)).$$

Corollary 4.6. *(cf.* [4, Corollary 2.5]*) A polynomial mapping $P : \mathbb{F}^n \to \mathbb{F}^m$ contains an (s,r)-elusive k-tuple, if and only if the subset*

$$\hat{P}^k := P(\mathbb{F}^n) \times_{k\,times} \times \subset \mathbb{F}^{mk}$$

does not belong to the image of the evaluation mapping $\bar{E}v^k_{s,r,m}$.

Proposition 4.5 and Corollary 4.6 are proved in the same way as [4, Lemma 2.4, Corollary 2.5], so we omit their proofs.

As in [4, Proposition 3.5] we can also apply the effective elimination theory to find concrete (s,r)-weakly elusive k-tuple, and using the interpolation formula in [4, Proposition 2.6] to construct concrete (s,r)-weakly elusive polynomial mappings, whose monomial coefficients are algebraic numbers.

Remark 4.7. Proposition 4.5 implies that if

$$k \geq \frac{\binom{s}{r} + 1}{m - s},$$

then there are a lot of k-tuples S_k of points in $\mathbb{F}^m$ which are (s,r)-weakly elusive. Hence, using the interpolation formula, as in [4, Proposition 2.6], it follows that there are many polynomial mappings $P \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ which are (s,r)-weakly elusive if

$$\binom{n+p}{p} \geq \frac{\binom{s}{r} + 1}{m - s}. \tag{4.7}$$

Proving that a polynomial mapping P contains an (s,r)-weakly elusive tuple of points is considerably more complicated than to estimate the dimension of the regular functions on the image of P, but it may yield non-trivial lower bounds for the circuit size of the permanent, see the next subsection.

4.3. **Geometry of the mapping $\tilde{g}^{n,t}$ associated to the permanent.** Let us keep the notation we use in section 3. In this subsection we study the geometry of the mappings $\tilde{g}^{n,t}$, which are sightly simpler than $g^{n,t}$, but might yield similar lower bounds for the circuit size of P_m as $g^{n,t}$.

Recall that Z is a rectangular matrix of size $(n-t)n$. Denote by $\bar{P}er(Z)$ the linear subspace of $Pol^{n-t}_{hom}(\mathbb{F}\langle Z\rangle)$ which is generated by the (minor) permanents of size $(n-t)\times(n-t)$ of the matrix Z. Clearly $\dim \bar{P}er(Z) = \binom{n}{n-t}$.

Lemma 4.8. *The linear span of $\tilde{g}^{n,t}(\mathbb{F}(\langle Y\rangle)$ is $\bar{P}er(Z)$. Hence $\tilde{g}^{n,t}$ is $(s,1)$-weakly elusive for $s = \binom{n}{n-t} - 1$.*

Proof. Lemma 4.8 is proved by observing that all the basis of $\bar{P}er(Z)$ lies on the image of $g^{n,t}$. □

Thus $\tilde{g}^{n,t}$ can be regarded as a polynomial mapping from $\mathbb{F}^{nt}$ into $\mathbb{F}^{\binom{n}{n-t}}$, and no further dimension reduction of the target space of $\tilde{g}^{n,t}$ is possible.

Let us speculate for which value (s,r) the map $\tilde{g}^{n,t}$ could be (s,r)-weakly elusive, and moreover, this value (s,r) would bring non-trivial lower bounds for the circuit size of P_n. Theorem 3.3 yields that, r must be equal to $2(n-t)-1$ (cf. Theorem 3.1). We also wish to have $s = n^\alpha$ where α should take large values in order to obtain a non-trivial lower bounds for $L(P_n)$. Since the degree of $\tilde{g}^{n,t}$ is t, Remark 4.7 asserts that, the value of $s = n^\alpha$ is only constrained by the following conditions

$$n^\alpha \leq \binom{n}{n-t} - 1, \tag{4.8}$$

$$\binom{nt+t}{t} \geq \frac{\binom{n^\alpha}{2(n-t)-1} + 1}{\binom{n}{n-t} - n^\alpha}. \tag{4.9}$$

The validity of (4.9) implies that, a "generic" polynomial mapping of degree t from $\mathbb{F}^{nt}$ to $\mathbb{F}^{\binom{n}{n-t}}$ is $(n^\alpha, 2(n-t)-1)$-weakly elusive. If α is much less than $n-t$ and $2(n-t)\alpha$ is much less than t then (4.8) and (4.9) surely hold. For instance, the values $n = 2^{2^k}$, $\alpha = 2^{2^{k-3}}$, $n-t = 2^{2^{k-2}}$ would satisfy the above constrain. In this case, if $\tilde{g}^{n,t}$ is "generic", the circuit size of the permanent P_n is bounded from below by $A\cdot \frac{n^{\alpha/2}}{(n-t)^3}$, where A is a (universal) constant which can be explicitly obtained from Theorem 3.1.

5. Appendix: Normal form of arithmetic circuits and universal circuit-graph

In this Appendix we reformulate a Raz's theorem on normal-homogeneous circuit (Theorem 5.4), making precise an estimate in his original assertion. Then we reformulate Raz's theorem on the existence of a universal circuit-graph (Proposition 5.5), improving a Raz's estimate. These estimates play important role in the previous sections.

First we recall some necessary definitions.

Definition 5.1. (cf. [7, §1.1]) *An arithmetic circuit* is a finite directed acyclic graph whose nodes are divided into four types: *an input-gate* is a node of in-degree 0 labelled with an input variable; *a simple gate* is a node of in-degree 0 labelled with the field element 1; *a sum-gate* is a node labelled with $+$; *a product-gate* is a node labelled with $\times$; *an output-gate* is node of out-degree 0 giving the result of the computation. Every edge (u, v) in the graph is labelled with a field element α. It computes the product of α with the polynomial computed by u. A product-gate (resp. a sum-gate) computes the product (resp. the sum) of polynomials computed by the edges that reach it. We say that a polynomial $f \in \mathbb{F}[x_1, \cdots, x_n]$ is computed by a circuit if it is computed by one of the circuit output-gates. If a circuit has m output-gates, then it computes an m-tuple of polynomials $f^i \in \mathbb{F}[x_1, \cdots, x_n]$, $i \in [1, m]$. The *fanin* of a circuit is defined to be the maximal in-degree of a node in the circuit, that is, the maximal number of children that a node has.

Definition 5.2. [7, §2] *A circuit-graph* G is the underlying graph G_Φ of an arithmetic circuit Φ together with the labels of all nodes. This is the entire circuit, except for the labels of the edges. We call $G = G_\Phi$ *the circuit graph* of Φ. The *size* of an arithmetic circuit Φ is defined to be the number of edges in Φ, and is denoted by $Size(\Phi)$. The *depth* of a circuit Φ is defined to be the length of the longest directed path in Φ, and is denoted by $Depth(\Phi)$. The *circuit size* $L(P)$ of a m-tuple P of polynomials $g_1, \cdots, g_m \in \mathbb{F}[x_1, \cdots, x_n]$ is the minimal size of an arithmetic circuit computing P.

Definition 5.3. [7, Definitions 2.1, 2.2] A circuit graph G_Φ is the underlying graph of an arithmetic circuit together with the labels of all nodes. A circuit graph G is called homogeneous, iff for every arithmetic circuit Φ such that $G = G_\Phi$ and every gate v in Φ, the polynomial computed by the gate v is homogeneous. Further, we say that a homogeneous graph is in normal form, if it satisfies

(1) All leaves are labelled by input variables (i.e. no leave is labelled by the field element 1).

(2) All edges from the leaves are to sum-gates.
(3) All output gates are sum-gates.
(4) The gates of G are alternating. That is, if v is a product-gate (resp. sum-gate) and (u, v) is an edge, then u is a sum-gate (resp. product-gate or a leaf.)
(5) The in-degree of every product-gate is exactly 2.
(6) The out-degree of every sum-gate is at most 1.

We say that an arithmetic circuit is in a normal-homogeneous form, if the circuit graph G_Φ is in a normal-homogeneous form.

Note that any ordered m-tuple of polynomials $g_1, \cdots, g_m \in \mathbb{F}[x_1, \cdots, x_n]$ can be considered as a polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^m$.

Theorem 5.4. *cf.* [7, Proposition 2.3] *Let Φ be an arithmetic of size s that computes an m-tuple P of homogeneous polynomials $g_1, \cdots, g_m \in Pol^r_{hom}(\mathbb{F}^n)$. Then there exists an arithmetic circuit Ψ for the polynomials $g_1, \cdots, g_m$ such that Ψ is in a normal homogeneous form and the number of the node is less than $32s \cdot (r+1)^2$.*

Proof. Theorem 5.4 differs from [7, Proposition 2.3] in two points. Firstly, Raz assumed that $m = n$. Secondly, instead of the estimate $32s \cdot (r+1)^2$ Raz used $O(s \cdot r^2)$. These differences are not essential. The proof presented here follows the Raz's algorithm in the proof of [7, Proposition 2.3] that transforms an arithmetic circuit Φ computing P into an arithmetic circuit Φ_{norm} in normal homogeneous form which satisfies the condition of Theorem 5.4.

Step 1. If a (sum or product) gate in Φ has in-degree 1, then we remove its and connect its only child directly to all its parents. The size of the new circuit is equal to the size of the old circuit. Hence we can assume that Φ has *no gate of in-degree 1.* (This property is necessary for the next step and needs not be preserved under later steps).

Step 2. We transform Φ to Φ_1 which satisfies *the condition (5)* of Definition 5.3 by replacing any product-gate of in-degree larger 2 by a tree of product-gates of in-degree 2, and any sum-gate of in-degree larger than 2 by a tree of sum-gates of in-degree 2. It is easy to check that $Size(\Phi_1) \leq 2s$.

Step 3. We transform Φ_1 to Φ_2 computing P such that G_{Φ_2} is *homogeneous and satisfying the condition (5).* The nodes of Φ_2 is obtained by splitting each node $v \in \Phi_1$ into $(r+1)$-nodes $v_0, \cdots, v_r$, where the node v_i computes the homogeneous part of degree i of the polynomial computed by the node v. We ignore monomials of degree larger than r. If (the original node) $v \in \Phi_1$ is a sum-gate, we replace the

sub-circuit in Φ_1 connecting v with its children u, w by the circuits that compute $v_i = u_i + w_i$ for all $i \in [0, r]$. If $v \in \Phi_1$ is a product-gate, we replace the sub-circuit in Φ_1 connecting v with its children u, w by the sub-circuits of that compute $v_i = \sum_{j=0}^{i} u_j \times w_{i-j}$ for all $i \in [0, r]$. Clearly Φ_2 also computes P, moreover Φ_2 is homogeneous, satisfies the condition (5) in Definition 5.3. It is easy to check that $Size(\Phi_2) \leq (r+1)^2 \cdot Size(\Phi_1) \leq 2(r+1)^2 s$.

Step 4. We transform Φ_2 to a homogeneous circuit Φ_3, that computes P and satisfies *the conditions (1), (5)* in Definition 5.3. Let $u \in \Phi_2$ be a node computing a field element α_u. We assume that u has out-degree at least 1, otherwise we remove u. Let v be a parent of u. If v is a sum-gate, noting that Φ_2 is homogeneous, v computes a field element α_v. Then we replace the sub-circuit computing v from its children by a leave labelled by 1 and multiply the labelled of all the edges from v by α_v. If v is a product-gate, then v has the only two children u and w, so we replace the sub-circuit consisting of v together with all edges connecting with v by edges connecting u and w with the parents of v. Repeating this process we get the desired circuit Φ_3 with $Size(\Phi_3) \leq Size(\Phi_2) \leq 2(r+1)^2 s$.

Step 5. We transform Φ_3 to a homogeneous circuit Φ_4 that computes P and satisfies *the conditions (1), (5) and (4).* This is done as follows. For any edge (u, v) such that u, v are both product-gates we add a dummy sum-gate in between them. For any edge (u, v) such that u, v are both sum-gates we connect all the children of u directly to u. Clearly $Size(\Phi_4) \leq 2Size(\Phi_3) \leq 4(r+1)^2 s$.

Step 6. We transform Φ_4 to a homogeneous circuit Φ_5 which computes P and satisfies *the conditions (1), (5), (4) and (3)* by connecting every product out-put gate to a new dummy sum-gate. Clearly $Size(\Phi_5) \leq 2Size(\Phi_4) \leq 8(r+1)^2 s$.

Step 7. We transform Φ_5 to a homogeneous circuit Φ_6 which computes P and satisfies *the conditions (1), (5), (4), (3) and (2)* by adding a dummy sum-gate in between any edge from a leave to a product gate. Clearly, $Size(\Phi_6) \leq 2Size(\Phi_5) \leq 16(r+1)^2 s$.

Step 8. We transform Φ_6 to a homogeneous circuit Φ_7 which computes P and satisfies all the conditions in Theorem 5.4 by duplicating q-times any sum-gate of out-degree $q > 1$. Clearly $Size(\Phi_7) \leq 2Size(\Phi_6) \leq 32(r+1)^2 s$.

This completes the proof of Theorem 5.4. □

Proposition 5.5. *cf.* [7, Proposition 2.8] *Assume that a quadruple (s, r, n, m) satisfies $n \leq s$, $1 \leq r$, and $m \leq 32s \cdot (r+1)^2$. Then there is a circuit-graph $G_{s,r,n,m}$, in a normal-homogeneous form that is*

universal for n-inputs and m-outputs circuits of size s that computes homogeneous polynomials of degree r, in the following sense.

Let $\mathbb{F}$ be a field. Assume that a polynomial mapping $P := (g_1, \cdots, g_m) \in Pol^r_{hom}(\mathbb{F}^n, \mathbb{F}^m)$ is of circuit size s. Then, there exists an arithmetic circuit Ψ that computes P such that $G_\Psi = G_{s,r,n,m}$.

Furthermore, the number of the edges leading to the sum-gates in $G_{s,r,n,m}$ is at most $2^8 s^2 r^2 (r+1)^4$.

Proof. This Proposition differs from Proposition 2.8 in [7] only in three instances. Firstly, Raz assumed that $m = n$. Secondly, we have a concrete, estimate on the number of edges leading to the sum-gates of $G_{s,r,n,m}$, which yields a better estimate on the degree of the associate polynomial mapping. For the case of the convenience of the reader we outline the proof of Proposition 5.5 here, referring the reader to [7] for more details. It is based on Theorem 5.4. The idea is to produce a circuit-graph $G_{s,r,n,m}$ with sufficient nodes and edges so that the circuit-graph of any normal-homogeneous circuit Φ computing P can be embedded into $G_{s,r,n,m}$.

The circuit-graph $G_{s,r,n,m}$ is constructed as follows. First, we divide the nodes of $G_{s,r,n,m}$ into $2r$-level. The first level contains the input-gates, and the last level contains the output-gates. Other even-numbered levels contain exactly $32s(r+1)^2$ sum-gates and odd-numbered levels contain product-gates. The level i contains gates of the same syntactic degree i. Furthermore, we partition the product-gates in level $(2i-1)$ into $(i-1)$ types. Each of these type contains exactly $16s(r+1)^2$ nodes. Thus we have at most $16s \cdot r(r+1)^2(r+2)$ nodes in $G_{s,r,n,m}$.

Now we describe the edges of $G_{s,r,n,m}$.

(1) The children of a sum-gate in level $(2i)$ are all the nodes in level $(2i-1)$.
(2) The two children of a product-gate of type i in level $(2i-1)$ are a sum-gate in level (2j) and a sum-gate in level $(2i-2j)$.

Using Theorem 5.4 we prove that $G_{s,r,n,m}$ is universal.

The last assertion of Proposition 5.5 follows from (1). This completes the proof of Proposition 5.5. □

For the case $r = 1$ we have a normal form theorem. Though the value m in Raz's paper is fixed to be equal n, but in fact he does need that condition in his proof. Hence we omit the proof of the Proposition below.

Proposition 5.6. *(cf. Definition 2.4, Proposition 2.5]Raz2009) Let $\mathbb{F}$ be a field. Let Φ be an arithmetic circuit of size s and depth d for a m linear polynomials $g_1, \cdots, g_m \in \mathbb{F}[x_1, \cdots, x_n]$. Then there exists an*

arithmetic circuit Ψ of size s and depth d for the polynomials $g_1, \cdots, g_m$ such that all nodes in G are either input-gates or sum-gates.

The circuit Ψ (resp. its circuit-graph) in Proposition 5.6 is called *in normal-linear-form.*

We end this appendix with the following remark on universal circuits, which is needed in the main body of our note.

Remark 5.7. ([7, 3.2]) Assume that Φ is a normal homogeneous arithmetic circuit that computes a polynomial $P \in Pol^r(\mathbb{F}^n, \mathbb{F}^m)$. Then there is an arithmetic circuit Ψ of the same circuit-graph as Φ that computes P such that the label of any edge leading to a product-gate in Ψ is 1.

Acknowledgements

The author would like to thank Pavel Pudlak for his stimulating discussions. A part of this paper has been conceived during the author's visit to VNU for Sciences in Hanoi and the ASSMS in Lahore-Pakistan. She would like to thank these institutions for excellent working conditions and financial support.

References

[1] W. Baur, V. Strassen, The Complexity of Partial Derivatives. Theor. Comput. Sci. 22(1983), 317-330.
[2] P. Burgisser, M. Clausen and M. A. Shokrollali, Algebraic Complexity Theory, Springer -Verlag, (1997).
[3] J. zur Gathen, Feasible Arithmetic Computations: Valiant's Hypothesis, J. Symbolic Computation (1987) 4, 137-172.
[4] H. V. Lê, Constructing elusive functions with help of evaluation mappings, arXiv:1011.2887
[5] T. Mignon and N. Ressayre, A quadratic bound for the Determinant and Permanent Problem, IMRN 79 (2004), 4241-4253.
[6] K.D. Mulmuley and M. Sohoni, Geometric complexity theory, I, An approach to the P vs. NP and related problems, SIAM J Computing 31 (2001), n.2 , 496-526.
[7] R. Raz, Elusive Functions and Lower Bounds for Arithmetic Circuits, Theory Of Computing Vol. 6, article 7 (2010).
[8] A. Shpilka and A. Yehudayoff, Arithmetic Circuits: a survey of recent results and open questions, Foundations and Trends in Theoretical Computer Science: Vol. 5: No 3-4, pp 207-388 (2010).
[9] L.G. Valiant, Completeness classes in algebra, Conference Record of the Eleventh Annual ACM Symposium on Theory of Computing (Atlanta, Ga, 1979), Association for Computing Machinery, New York, (1979), p. 249-261.

[10] L. G. Valiant, Reducibility by Algebraic Projections. In Logic and Algorithmic: an International Symposium held in honor of Ernst Specker, volume 30 of Monographies de lEnseignement Mathemathique, (1982), 365-380.

Institute of Mathematics of ASCR, Zitna 25, 11567 Praha, email: hvle@math.cas.cz